AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

UNITED STATES OF AMERICA
Plaintiff
v.
STATE OF GEORGIA
Defendant

Civil Action No. 1:16-CV-03088-ELR

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: OCONEE CENTER COMMUNITY SERVICE BOARD
131 North Jefferson St.
Milledgeville, GA 31061

(Name of person to whom this subpoena is directed)

✔ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material:

Place: Electronic Production via the United States' secure filesharing system, JEFS, or through other means with agreement from counsel for the United States	Date and Time: 9/6/2022 11:59 pm

Inspection of Premises: **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting partymay inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it as set forth in Attachment A hereto.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 8/15/2022

CLERK OF COURT

Signature of Clerk or Deputy Clerk

OR

Aileen Bell Hughes

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* the United States of America, who issues or requests this subpoena, are:

Aileen Bell Hughes, 75 Ted Turner Dr. SW, Suite 600, Atlanta, GA 30303; aileen.bell.hughes@usdoj.gov; 404-581-6133

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 1:16-CV-03088-ELR

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

’ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

’ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day’s attendance, and the mileage allowed by law, in the amount of

$ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____ _____

Server’s signature

_____

Printed name and title

_____

Server’s address

Additional information regarding attempted service, etc.:

Print Save As... Add Attachment Reset

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

ATTACHMENT A

Pursuant to Fed. R. Civ. P. 45(a)(1)(C), (D), OCONEE CENTER COMMUNITY SERVICE BOARD is commanded to produce by September 6, 2022, the designated documents, electronically stored information, or tangible things in its possession, custody, or control as identified below.

INSTRUCTIONS

1. This subpoena covers all documents in or subject to your possession, custody, or control, including all documents that are not in your immediate possession but that you have the effective ability to obtain and that are responsive, in whole or in part, to any of the individual requests set forth below. If for any reason—including a claim of attorney-client privilege—you do not produce documents called for by this subpoena, you should submit a list of the documents you are not producing. The list should describe each document in a manner that, without revealing information itself privileged or protected, will enable the United States to assess the claim of privilege. This description should include the following: the author of the document, date of the document, recipient(s) of the document, subject matter of the document, each person who has ever possessed a copy of the document, the basis for withholding the document, the attorney(s) and client(s) involved (if applicable), and the subpoena request to which the document is responsive.

2. Unless otherwise specified, these requests seek responsive documents from the 2019-20 fiscal year ("FY2020") through the 2021-22 fiscal year ("FY2022").

3. If documents responsive to this subpoena no longer exist because they have been lost, discarded, or otherwise destroyed, you should identify each such document, the date on which it was lost, discarded, or destroyed, and the reason(s) for its loss, discarding, or destruction.

4. Documents should be produced as they are kept in the ordinary course of business. Documents created or stored electronically must be produced in their native electronic format, not printed to paper. All documents should be produced in a unitized manner (i.e., separated or otherwise delineated to identify the boundaries for each document).

5. Data should be produced in a searchable and usable electronic format. Specifically, for any request for a collated list of data, please provide the information using a Microsoft Excel spreadsheet, with the delineated data separated by appropriate columns and rows. Please also

provide a corresponding data dictionary/key. For any request for copies of documents, please provide the information as a searchable Word or Adobe Acrobat file. To the extent any information is available online, please provide the URL address(es) where the information is located.

6. All documents produced should be labeled with sequential numbering (Bates-stamped). The Bates stamps should begin with a letter prefix that identifies the CSB and that prefix should be followed by numbering that includes at least six digits (e.g., "ABC000001").

7. For any documents that qualify as records of regularly conducted activities under Federal Rule of Evidence 902(11), please complete a business records certification (a sample of which is enclosed) and return it with the document production.

DEFINITIONS

As used in this subpoena, the words and phrases listed below shall have the following meanings:

1. For purposes of responding to this subpoena, "you" means OCONEE CENTER COMMUNITY SERVICE BOARD, its constituent agencies or facilities, and any of its officers, employees, contractors, attorneys, representatives, investigators, agents, or any other person acting or purporting to act on its behalf.

2. The Georgia Apex Program, or Apex, means the program identified as such by the Georgia Department of Behavioral Health and Developmental Disabilities (DBHDD) (e.g., https://dbhdd.georgia.gov/georgia-apex-program).

3. Community Service Board, or CSB, means any of the organizations so identified by the DBHDD (e.g., https://dbhdd.georgia.gov/locations/community-service-board).

4. "Document" means writings, electronic mail, drawings, graphs, charts, photographs, sound recordings, images, and other data, data records, or data compilations stored in any medium from which information can be obtained.

5. "Policies" or "procedures" means any written or unwritten policy, procedure, manual, guidance, protocol, directive, mandate, rule, regulation, course of action, strategy, plan, guiding principle, guidelines, method, routine, process, modus operandi, technique, practice, system, formula, routine, or other mode of conduct that governs operations.

6. "Behavioral health service" means any service listed by DBHDD in its Community Behavioral Health Provider Manual for the relevant Fiscal Year as a "child and adolescent non-intensive outpatient service" or "child and adolescent specialty service," excluding the Apex Program.

7. The present tense includes the past and future tenses. Words in the singular and plural are interchangeable. The terms "all" and "any" mean "any and all;" "and" and "or" encompass both "and" and "or." The word "including" means "including, but not limited to."

DOCUMENTS

Oconee Center Community Service Board Overview

1. For FY2020, FY2021, and FY2022, an organizational chart by name & position, capturing: (1) Executive Leadership; (2) child and adolescent services staff; and (3) Apex program staff (where applicable)

2. A copy of OCONEE CENTER COMMUNITY SERVICE BOARD's most recent strategic plan(s)

3. Monthly, quarterly, and annual progress/status reports, programmatic reports, or other tracking materials related to the strategic plan for the past three years

4. List(s) of both external and internal clinical trainings for child and adolescent Apex staff over the past two years, identifying: (1) topic of the training; (2) the OCONEE CENTER COMMUNITY SERVICE BOARD staff (child and adolescent/Apex) who attended each training; (3) who delivered the training (name, position, organization); and (4) who organized/sponsored the training.

Apex Contracts and Reporting

1. Contracts and related documents for Apex for Y6 (2020-2021) and Y7 (2021-2022)

2. All Apex monthly reports, specifically including progress and programmatic reports, for Y6 and Y7

Apex Schools, Services, and Staff

1. For each Medicaid billable and non-billable service provided through Apex, documents showing the school(s) where the service is provided; the settings where the service is provided (school, clinic, community, or home); and whether the service is provided during the school year only, during the summer only, or all year long

2. For Y6 and Y7, a list of staff who provided Apex services during these periods, including name, certification, service(s) provided, and dates of service provision (e.g., 09/21 to present)

Non-Apex Services and Staff

1. For each behavioral health service provided to children in an educational setting other than through Apex, documents showing the school(s) where the service is provided; the settings where the service is provided (school, clinic, community, or home); and whether the service is provided during the school year only, during the summer only, or all year long.

2. For School Years 2020-2021 and 2021-2022, a list of staff who provided behavioral health services to children in an educational setting other than through Apex, including name, certification, service(s) provided, and dates of service provision (e.g., 09/21 to present)

Types of assessments used

1. Copies of all current assessments or screening protocols/forms/template documents, whether formal or informal, relating to children's social/behavioral/emotional functioning

2. Documents showing the number of assessments and screenings performed relating to children's social/behavioral/emotional functioning, by assessment or screening

Progress monitoring relating to services/outcomes

1. Copies of all current protocols/tools for monitoring social/behavioral/emotional functioning and progress (including relating to discipline) – e.g., the Child and Adolescent Needs and Strengths ("CANS") tool – and related written policies

2. Any aggregate data or reporting relating to progress monitoring, by service, of child/adolescent social/behavioral/emotional functioning

CERTIFICATION OF AUTHENTICITY OF RECORDS OF REGULARLY CONDUCTED BUSINESS ACTIVITY

Pursuant to Rule 902(11) of the Federal Rules of Evidence, the undersigned declarant hereby declares, certifies, verifies or states under penalty of perjury the following:

1. The declarant is a records custodian or other qualified person who can provide a written declaration regarding the records of regularly conducted business activity which are the subject of this certification;

2. The records of regularly conducted business activity (hereinafter "records") which are the subject of this certification are numbered/Bates stamped as _____ through _____;

3. The records are originals or duplicate copies of domestic (United States) business records, which are true and correct copies of the original record(s) prepared and/or maintained by _____[CSB Program];

4. The records were made at or near the time of the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

5. The records were kept in the course of a regularly conducted business activity; and

6. The records were made as a regular practice in the course of regularly conducted business activity.

I hereby declare, certify or state, under penalty of perjury, that the foregoing is true and correct. Executed on _____ (date)

_____
Signature of Declarant

_____
Printed Name

_____
Title

_____
CSB Program Name

_____
Address

_____
Telephone

Account Request and Approval Form

Non-Civil Rights Division User

JEFS Account Request Form for External non-DOJ Users

Account Type:	◉ User (JEFS - Application Users)	JEFS is strictly for Department of Justice (DOJ) official business.

DOJ Staff Name (Sponsor)	Date of Request
Megan Erickson	08/15/2022

Request Type: User Account	◉ Grant or Modify Access	○ Remove Access
Request Type: Folder	◉ Grant or Modify Access	○ Remove Access

NOTE:

Please include any additional information here. (special instructions, folder name(s), etc.)

Folder Name -
GNETS - Oconee Center Community Service Board

External User Information			To be checked by Account User:
First Name	Middle Initial	Last Name	☐ I have read and agree to abide by the Rules of Behavior as described in the attached pages.

Organization / Company	Email Address

Address (Street, City, State)	Zip code

Sponsoring Component	Citizenship of (Country)	Phone Number
Civil Rights Division, Educational Opportunities Section		

Approving Official (Component DSO or Manager)	
Name (Print or Type)	Title
Approver Signature	

Approving Official JEFS (To be signed by JEFS Support Team)	
Name (Print or Type)	Title
Approver Signature	

JEFS Account Request Form for External non-DOJ Users

Terms and Conditions

Department of Justice (DOJ), Civil Rights Division Terms and Conditions for JEFS Users

Introduction

The intent of the Terms and Conditions is to summarize for you, a user of DOJ Information Technology resources, the applicable laws and requirements from various Federal and DOJ documents. These include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, OMB M-17-12, OMB M-16-24, DOJ Order 2640.2 (series), DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

To remain compliant with all applicable Federal laws, regulations, and DOJ Standards, the Department reserves the right to update these terms and conditions at any time. Please direct all questions relating to the terms and conditions to your Point of Contact (POC) or the Litigation Support Group Case Manager.

Who is covered by these rules?

These rules apply to Litigation Consultants, Expert Witnesses, Mediators, and Non-Civil Rights Division Users providing services to DOJ. They also apply to any other persons using DOJ Information Technology or accessing DOJ systems under formally established agreements. These rules are written for the vast majority of people for the vast majority of time. However, some people (e.g. Investigators) may be exempt from a specific item for a specific situation when performing their official duties and with proper authorization. In a similar manner, equipment and/or software limitations may prevent operation in accordance with some of these rules.
These situations must be documented, the risks accepted, and the applicable processes approved by the system Authorizing Official. All users are required to review and provide signature or electronic verification acknowledging compliance with these rules.

What are the penalties for noncompliance?

Non-compliance with requirements will be enforced through sanctions commensurate with the infraction. Actions and penalties may include a verbal or written warning, temporary suspension of system access, permanent revocation, civil, criminal, financial, and imprisonment depending on the severity of the violation. (We will not deal with any classified information)

Unauthorized browsing or inspection of Federal Taxpayer Information (Internal Revenue Code Sec. 7213A) is punishable with a fine of up to $1,000 and/or up to one year imprisonment. Unauthorized disclosure of Tax Return information (Internal Revenue Code Sec. 7213) is a felony punishable with a fine of up to $5,000 and/or up to five years in prison. In addition to these penalties, any Federal employee convicted under Sec. 7213 or Sec. 7213A will be dismissed from employment.

JEFS Account Request Form for External non-DOJ Users

User Security Guide

Your responsibilities as an external user:

1. Comply with all Federal laws and Department and Component policies and requirements. Use DOJ information and information systems for lawful, official use, and authorized purposes only.
2. Read and accept the DOJ security warning banner that appears prior to logging onto the system.
3. Screen-lock or log off your computer when JEFS is no longer in use.
4. Do not post Department information on cloud-based services unless approved.
5. Do not post Department information for official business on public websites or social media unless explicitly authorized for your official duties. (e.g., Public Affairs Office)
6. Do not post information on social media or public websites that allows unauthorized users to infer or obtain non-public information (system account information, personal identifiable information (PII), project status, etc.).
7. Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all PII being sent to third parties.
8. Protect and safeguard all DOJ information and information systems from unauthorized access; unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service; and improper sanitization or use.
9. JEFS users shall ensure that all DOJ data are stored on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) is encrypted with a Department-approved solution unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.
10. Handle all Department data as Sensitive unless designated as non-Sensitive by your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager.
11. Report any anomalous or unusual behavior, and discovered or suspected security incidents to your appropriate point of contact (POC) (e.g., Civil Rights Attorney, Litigation Support Group (LSG) Case Manager, LSG Office at 202-514-4224, or Justice Security Operations Center [JSOC], DOJCert@usdoj.gov).
12. The email address associated with your JEFS account should be attributable by another party or organization (e.g., .org, .com, .mil, .gov) controlled by only you and not shared with anyone, even family members.
13. Do not attempt to circumvent or test the security controls of the system.

JEFS Account Request Form for External non-DOJ Users

Passwords

14. Change the default password upon receipt from a system administrator.

15. Do not share account passwords with anyone.

16. Avoid using the same password for multiple accounts.

Software

17. Do not copy or distribute intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials). Use DOJ-licensed and authorized software only.

18. Do not install or update software on the File Sharing System unless specifically authorized.

19. Do not attempt to access any electronic audit trails that may exist on the File Sharing System computer.

At the completion of your service, please properly dispose of any case related data Contact your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager for more guidance.

Mobile Computing & Remote Access

20. When utilizing the Litigation Support System, connect to a secure wireless network (password protected) and take precautionary measures to prevent the compromise of DOJ data when insecure wireless networks must be used. **Never connect to open wireless networks that require no passwords.**

21. Ensure the confidentiality of government information from a non-Government Furnished Equipment (GFE) client (public or private). This includes the following:

    a. Non-GFE devices and computers must have updated antivirus, local firewall, updated Operating System security patches and software patched levels.

    b. In addition, all wireless access to DOJ networks must be from a WI-FI Protected Access 2 (WPA2) or higher encrypted wireless network with password protection.

    c. Do not download documents or files public computers.

    d. Purge documents and files when finished on a non-GFE private will be held responsible for the compromise of Government information through negligence or a willful act.

JEFS Account Request Form for External non-DOJ Users

Personally Identifiable Information (PII)

22. Verify that each computer-readable data extract containing sensitive PII data has been erased within 90 days of origination or that its use is still required. Contact your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager.

23. Safeguard against breaches of information involving PII, which refers to information that can be used alone or combined with other information that can distinguish or trace an individual's identity --such as a name, social security number, biometric records, the date and place of birth, mother's maiden name, etc.

24. Report all breaches of information involving PII to your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager as soon as possible.

Signature Block

I acknowledge receipt of, understand my responsibilities as identified in, and will comply with the DOJ Civil Rights Division Terms and Conditions for External Users. This includes my responsibility to ensure protection of PII that I may handle.

Your Signature	Date
	DOJ CRT EOS
Your Printed Name	Organization/Component

[*Note: For DOJ employees, statement of acknowledgement may be made by signature of the Terms and Conditions for General Users are provided in hard copy or by email.]*

JEFS Account Request Form for External non-DOJ Users

Confidentiality Agreement

In consideration of being provided access to the Department of Justice (DOJ), Civil Rights Division Justice Enterprise File Sharing System (JEFS), the User hereby agrees to the following:

1. The provisions of this agreement shall apply to and be binding upon the User, the User's company, business, employees, agents, officers, successors and assigns, and any person acting upon behalf of the User in relation to the DOJ case(s) or project(s) he or she is authorized to access.

2. Except as required by law, as otherwise provided in this agreement, or as directed in writing by the Department of Justice, no information obtained, developed, gathered, or created as a result of work performed in connection with this matter, including any training materials or guidance concerning the System, shall be provided or disclosed orally, in writing, or in any other form, including the transmission of electronic data, to any third party or person who is not a part of this agreement. In any case in which disclosure of such information is or may be appropriate, no disclosures shall be made without prior written approval of the Department of Justice. This prohibition includes, but is not limited to communications with any person representing the media, any industry representatives, and any colleagues or fellow researchers. Disclosures may be made to persons who have signed and filed Confidentiality Agreements with the Department of Justice in connection with this case or project, as well as your management, supervisory, or support personnel as they may be necessary to execute your role as an authorized User in connection with this case or project.

3. Except as required by law, as otherwise provided in this agreement, or as directed by the Department of Justice, all documents, information, electronic data, or other work obtained, developed, gathered, or created as a result of System access, including documents or other information provided by the United States or other parties, shall be treated as privileged Sensitive But Unclassified (SBU) information. The User shall not reveal such materials to any third party or person without prior written approval from the Department of Justice, except for those persons who have signed and filed Confidentiality Agreements with the Department of Justice in connection with this case or project.

4. Should any documents, information, or electronic data, provided, obtained, developed, gathered, or created in connection with this System be lost, discovered missing, or mistakenly or inadvertently turned over without DOJ consent to an unauthorized person or third party, the User shall immediately report the details of such incident to the lead Department of Justice attorney point of contact responsible for this case or matter and the Litigation Support Group (LSG) Case Manager assigned to this case or project. In the event the User receives any requests in any form for such information, the User shall immediately notify the lead Department of Justice attorney point of contact and LSG Case Manager and await and follow DOJ instructions on how to proceed.

5. The User is responsible for notifying the LSG Case Manager when his or her involvement in this case or matter has concluded, at which time the User will request termination of access to the System. The User shall deliver upon request, within 30 days of notification that System access has been terminated, all documents, electronic data, and other information provided, obtained, developed, gathered, or created in connection with System access and related to the case or project he or she was supporting to the Department of Justice.

6. Notwithstanding the terms of this agreement, documents created by third-parties and gathered as evidence in litigation that are stored as images on the System will not be deemed to be privileged or confidential by virtue of this agreement. Nothing in this agreement limits the authority of agents or attorneys assigned to the matters in which that evidence is, was or will be collected from disclosing that evidence to witnesses, courts, or other persons who are not parties to this agreement in any manner authorized by law as necessary for those assigned agents and attorneys to discharge their duties in investigating and prosecuting the matters.

Should you have any questions regarding these documents or your responsibilities, please contact your Litigation Support Group Case Manager.

Acknowledgement Block

I acknowledge receipt of the "CIVIL RIGHTS DIVISION, JUSTICE ENTERPRISE FILE SHARING SERVER User Security Guide & Confidentiality Agreement" and understand my responsibilities as identified. This includes my responsibility to ensure the protection of PII that I may handle.

Your Signature _____ Date _____

Your Printed Name _____

DOJ CRT EOS

Organization/Component

Account Request and Approval Form

Non-Civil Rights Division User

JEFS Account Request Form for External non-DOJ Users

Privacy Statement

In order for the Department of Justice Civil Rights Division to provide you with access to its document review system, please complete the attached form. Information gathered from this form will be used solely to confirm the identity and eligibility of the individuals requesting access to the system owned by the Civil Rights Division of the United States Department of Justice. Email, phone and computer information gathered will be used solely to create an account that will let the individuals requesting access view, process and/or store electronic information that is the property of the Civil Rights Division.

Failure to provide this information will result in denial of access to the document review system.

This form is not an application for Government employment. Information collected by this form will not be used for or affect any subsequent application for employment with the Federal Government.

The Department of Justice does not collect or use information for commercial marketing.

Information gathered in this form will not be disclosed outside of the Civil Rights Division except where contractors are acting on behalf of the Civil Rights Division, and where the Division may be required by law to disclose information you submit with other agencies for law enforcement purposes in accordance with the Civil Rights Division's routine uses published at 68 Fed. Reg. 47610 (Aug. 11, 2003, http://edocket.access.gpo.gov/2003/pdf/03- 20342.pdf) or to protect the Division from security threats.

Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules of the National Archives and Records Administration, and in some cases may be covered by the Privacy Act and subject to the Freedom of Information Act (FOIA). A discussion of the FOIA can be found at http://www.justice.gov/oip/foia_guide09.htm and a discussion about the Privacy Act can be found at http://www.justice.gov/opcl/privacyact1974.htm.

I acknowledge receipt of these Terms and Conditions and understand my responsibilities as identified in the DOJ Terms and Conditions. This includes my responsibility to ensure protection of PII that I may handle.

Signature _____ Date _____

Printed Name _____

DOJ CRT EOS

Component and Office

Clear Form Print Form